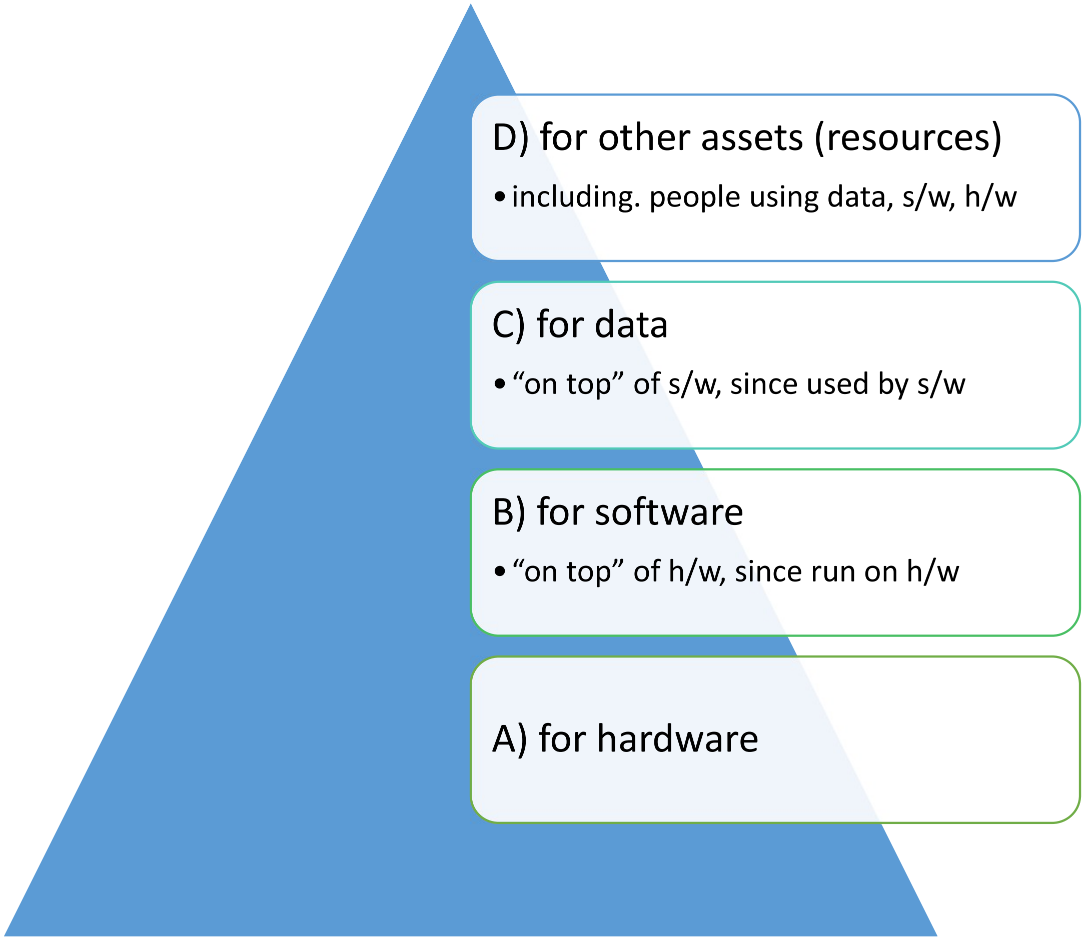
Vulnerabilities and Threats

Dr. Bhaskar Mondal

Threats are evolving to be more and more complex

Levels of Vulnerabilities / Threats



D) for other assets (resources)

- including. people using data, s/w, h/w

C) for data

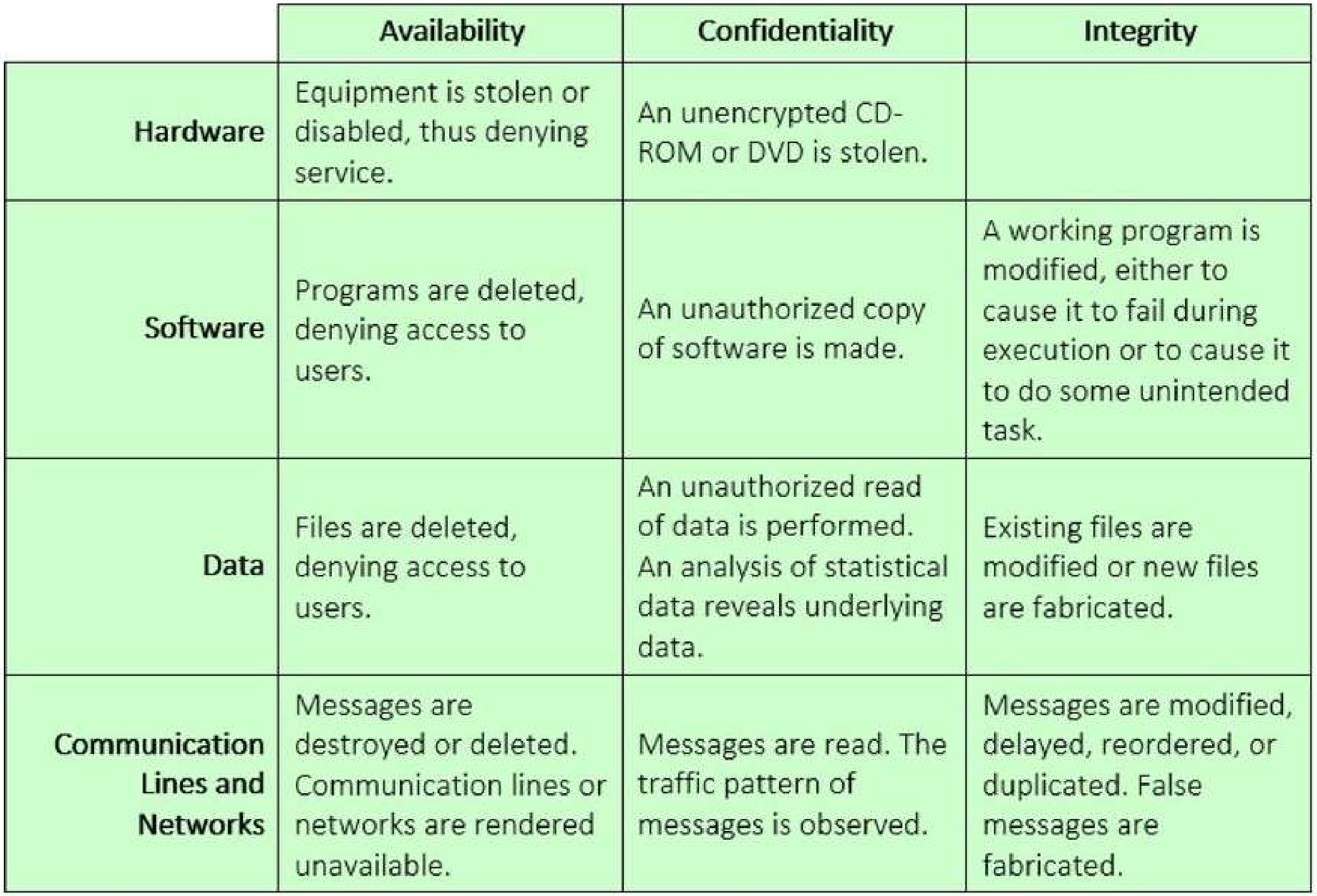
- “on top” of s/w, since used by s/w

B) for software

- “on top” of h/w, since run on h/w

A) for hardware

Threats



	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted CD-ROM or DVD is stolen.	
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines and Networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

A) Hardware Level of Vulnerabilities / Threats

- Add / remove a h/w device
  - Ex: Snooping, wiretapping

    Snoop = to look around a place secretly in order to discover things about it or the people connected with it. [Cambridge Dictionary of American English]
  - Ex: Modification, alteration of a system

- Physical attacks on h/w => need physical security: locks and guards
  - Accidental (dropped PC box) or voluntary (bombing a computer room)
  - Theft / destruction
    - Damage the machine (spilled coffe, mice, *real* bugs)
    - Steal the machine
    - “Machinicide:” Axe / hammer the machine

Physical security has three important components

access control

surveillance and

testing

Example of Snooping:
Wardriving / Warwalking, Warchalking,

Wardriving/warwalking: driving/walking around with a wireless-enabled notebook looking for unsecured wireless LANs

Warchalking: using chalk markings to show the presence and vulnerabilities of wireless networks nearby

E.g., a circled "W” -- indicates a WLAN protected by Wired Equivalent Privacy (WEP) encryption

[Barbara Edicott-Popovsky and Deborah Frincke, CSSE592/492, U. Washington]

B) Software Level of Vulnerabilities / Threats

Software Deletion

- Easy to delete needed software by mistake
- To prevent this: use *configuration management software*

Software Modification

- Trojan Horses, , Viruses, Logic Bombs, Trapdoors, Information Leaks (via covert channels), ...

Software Theft

- Unauthorized copying
  - via P2P, etc.

Types of Malicious Code

- **Bacterium:** A specialized *form of virus* which does not attach to a specific file. Usage obscure.
- **Logic bomb:** Malicious *[program] logic* that *activates when specified conditions are met*. Usually intended to cause denial of service or otherwise damage system resources.
- **Trapdoor:** A hidden *computer flaw known to an intruder*, or a hidden computer mechanism (usually software) installed by an intruder, *who can activate the trap door to gain access* to the computer without being blocked by security services or mechanisms.

[cf. http://www.ietf.org/rfc/rfc2828.txt]

Types of Malicious Code

- **Trojan horse:** A computer *program that appears to have a useful function*, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.
- **Virus:** A hidden, *self-replicating section of computer software*, usually malicious logic, that *propagates by infecting* (i.e., inserting a copy of itself into and *becoming part of) another program*. A virus cannot run by itself; it requires that its host program be run to make the virus active.
- **Worm:** A computer *program* that can run independently, *can propagate a complete working version of itself* onto other hosts on a network, and may consume computer resources destructively.

- More types of malicious code exist…

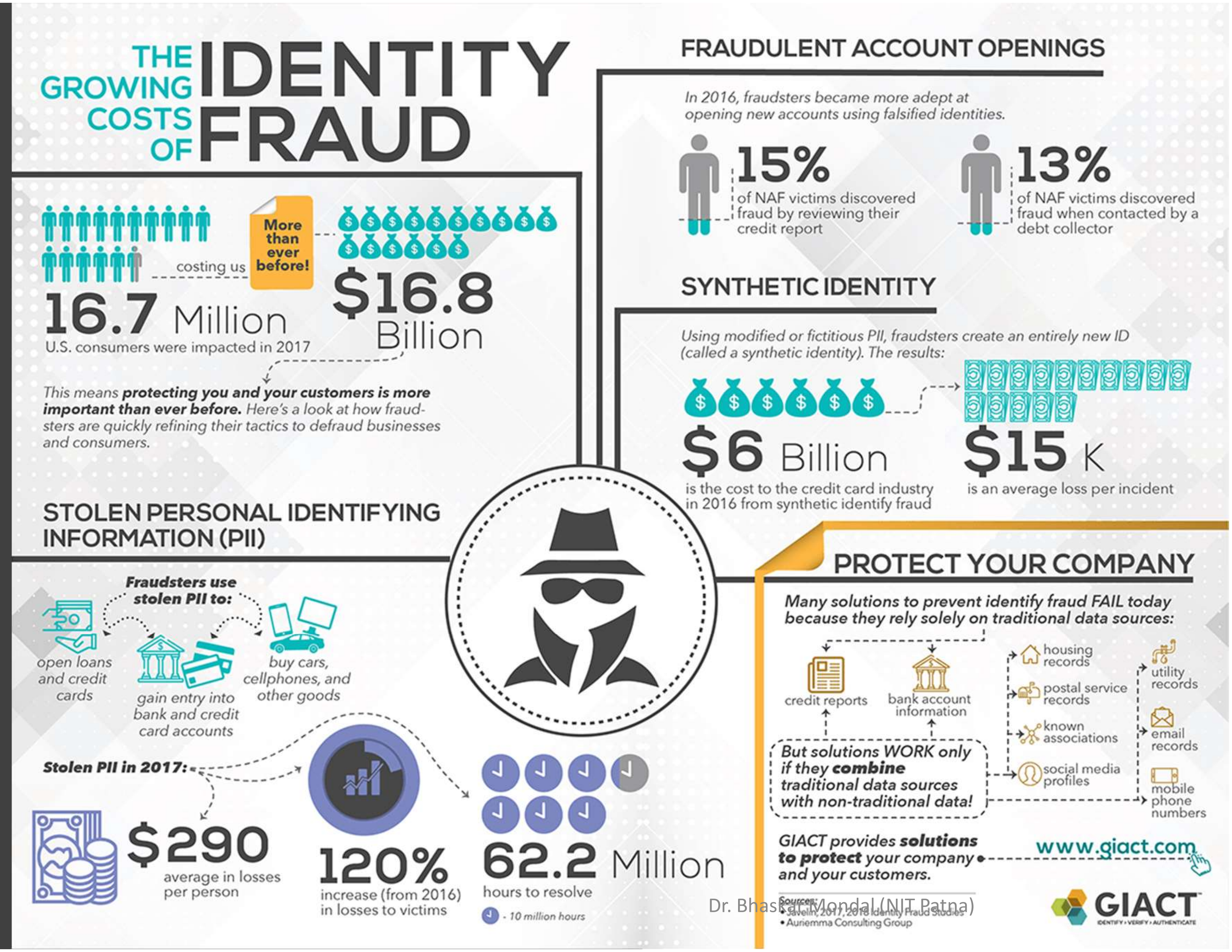
[cf. http://www.ietf.org/rfc/rfc2828.txt]

C) Data Level of Vulnerabilities / Threats

- How valuable is your data?
  - Credit card info vs. your home phone number
  - Source code
  - Visible data vs. context
    - “2345” -> Phone extension or a part of SSN?

- Adequate protection
  - Cryptography
    - Good if intractable for a long time

- Threat of Identity Theft
  - Cf. Federal Trade Commission: http://www.consumer.gov/idtheft/ \



THE GROWING COSTS OF IDENTITY FRAUD

16.7 Million U.S. consumers were impacted in 2017

costing us

More than ever before!

$16.8 Billion

This means **protecting you and your customers is more important than ever before.** Here's a look at how fraudsters are quickly refining their tactics to defraud businesses and consumers.

FRAUDULENT ACCOUNT OPENINGS

In 2016, fraudsters became more adept at opening new accounts using falsified identities.

15% of NAF victims discovered fraud by reviewing their credit report

13% of NAF victims discovered fraud when contacted by a debt collector

SYNTHETIC IDENTITY

Using modified or fictitious PII, fraudsters create an entirely new ID (called a synthetic identity). The results:

$6 Billion is the cost to the credit card industry in 2016 from synthetic identify fraud

$15 K is an average loss per incident

STOLEN PERSONAL IDENTIFYING INFORMATION (PII)

Fraudsters use stolen PII to:

open loans and credit cards

gain entry into bank and credit card accounts

buy cars, cellphones, and other goods

Stolen PII in 2017:

$290 average in losses per person

120% increase (from 2016) in losses to victims

62.2 Million hours to resolve

● - 10 million hours

PROTECT YOUR COMPANY

Many solutions to prevent identify fraud FAIL today because they rely solely on traditional data sources:

credit reports

bank account information

But solutions WORK only if they **combine** traditional data sources with non-traditional data!

housing records

postal service records

known associations

social media profiles

utility records

email records

mobile phone numbers

GIACT provides **solutions to protect** your company and your customers.

www.giact.com

Sources:
- Javelin, 2017, 2018 Identity Fraud Studies
- Auriemma Consulting Group

GIACT IDENTIFY • VERIFY • AUTHENTICATE

- According to Javelin Strategy & Research's, 15.4 million consumers in the U.S. were victims of identity theft in 2016 at an estimated cost of $16 billion.
- Federal Trade Commission: http://www.consumer.gov/idtheft/

D) Vulnerab./Threats at Other Exposure Points

- Network vulnerabilities / threats
  - Networks multiply vulnerabilties and threats, due to:
    - their complexity => easier to make design/implem./usage mistakes
    - „bringing close” physically distant attackers
  - Esp. wireless (sub)networks

- Access vulnerabilities / threats
  - Stealing cycles, bandwidth
  - Malicious physical access
  - Denial of access to *legitimate* users

- People vulnerabilities / threats
  - Crucial weak points in security
    - too often, the *weakest* links in a security chain
  - Honest insiders subjected to skillful social engineering
  - Disgruntled employees

5. Attackers need MOM

- Method
  Skill, knowledge, tools, etc. with which to pull off an attack

- Opportunity
  Time and access to accomplish an attack

- Motive
  Reason to perform an attack

Types of Attackers

- Types of Attackers - Classification 1
  - Amateurs
    - Opportunistic attackers (use a password they found)
    - Script kiddies
  - Hackers - nonmalicious
    - In broad use beyond security community: also, malicious
  - Crackers – malicious
  - Career criminals
  - State-supported spies and information warriors

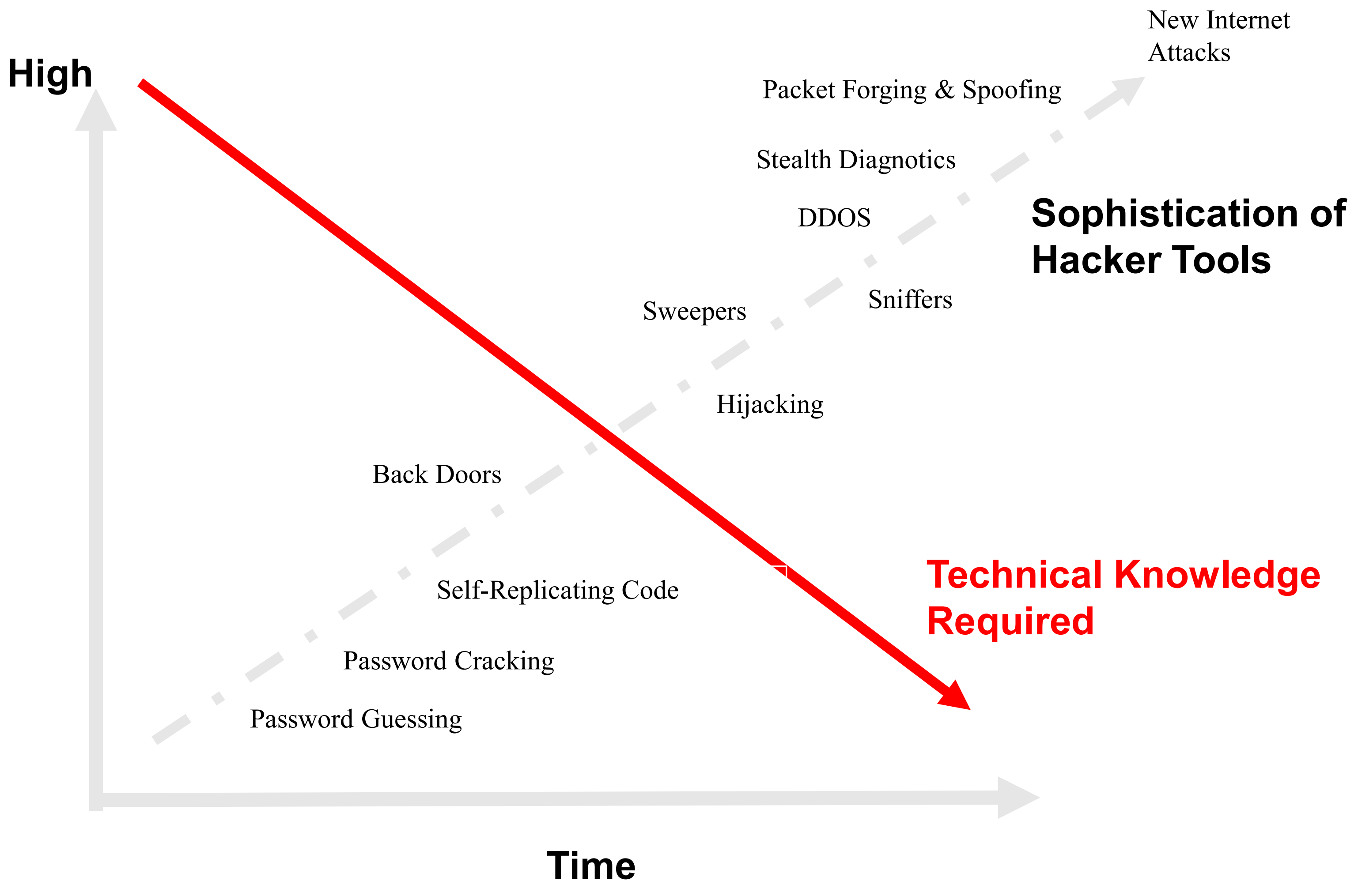
Types of Attackers

- Types of Attackers - Classification 2 (cf. before)
  - Recreational hackers / Institutional hackers
  - Organized criminals / Industrial spies / Terrorists
  - National intelligence gatherers / Info warriors

Example: Hacking As Social Protest

- Hactivism
- Electro-Hippies
- DDOS attacks on government agencies
- SPAM attacks as “retaliation”

- [Barbara Edicott-Popovsky and Deborah Frincke, CSSE592/492, U. Washington]



High

New Internet Attacks

Packet Forging & Spoofing

Stealth Diagnotics

DDOS

Sophistication of Hacker Tools

Sweepers

Sniffers

Hijacking

Back Doors

Technical Knowledge Required

Self-Replicating Code

Password Cracking

Password Guessing

Time

[Barbara Edicott-Popovsky and Deborah Frincke, CSSE592/492, U. Washington]

React to an Exploit

- Exploit = successful attack
- Report to the vendor first?
- Report it to the public?

  What will be public relations effects if you do/do not?
- Include source code / not include source code?
- Etc.

“To Report or Not To Report:” Tension between Personal Privacy and Public Responsibility

- An info tech company will typically lose between ten and one hundred times more money from shaken consumer confidence than the hack attack itself represents if they decide to prosecute the case.

--Mike Rasch, VP Global Security, testimony before the Senate Appropriations Subcommittee, February 2000 reported in The Register and online testimony transcript

[Barbara Edicott-Popovsky and Deborah Frincke, CSSE592/492, U. Washington]

Further Reluctance to Report

- One common fear is that a crucial piece of equipment, like a main server, say, might be impounded for evidence by over-zealous investigators, thereby shutting the company down.
- Estimate: fewer than one in ten serious intrusions are ever reported to the authorities.
- Mike Rasch, VP Global Security, testimony before the Senate Appropriations Subcommittee, February 2000
- reported in The Register and online testimony transcript

- Barbara Edicott-Popovsky and Deborah Frincke, CSSE592/492, U. Washington]